TIBCO Spotfire® Automation Services Installation and Configuration

Software Release 7.0
February 2015

Updated March 2015

Two-Second Advantage®

Important Information

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. SEE THE README FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

Contents

TIBCO Spotfire Automation Services Documentation and Support Service

All TIBCO documentation is available on the TIBCO Documentation site, which can be found here:

https://docs.tibco.com

Product-Specific Documentation

The following documents for this product can be found in the TIBCO Documentation Library for TIBCO Spotfire Automation Services:

- *TIBCO Spotfire® Automation Services User's Manual*
- *TIBCO Spotfire® Automation Services Installation and Configuration Manual*
- *TIBCO Spotfire® Automation Services License Agreement*

Product System Requirements

For a list of system requirements for this product and other TIBCO Spotfire® products, visit this site:

http://support.spotfire.com/sr_spotfire_main.asp

How to Contact TIBCO Support

For comments or problems with this manual or the software it addresses, contact TIBCO Support as follows:

- For an overview of TIBCO Support, and information about getting started with TIBCO Support, visit this site:

  http://www.tibco.com/services/support

- If you already have a valid maintenance or support contract, visit this site:

  https://support.tibco.com

  Entry to this site requires a user name and password. If you do not have a user name, you can request one.

How to Join TIBCOmmunity

TIBCOmmunity is an online destination for TIBCO customers, partners, and resident experts. It is a place to share and access the collective experience of the TIBCO community. TIBCOmmunity offers forums, blogs, and access to a variety of resources. To register, go to:

https://www.tibcommunity.com

Prerequisites

Before you install TIBCO Spotfire® Automation Services web service, you must meet the system requirements, and you must install and configure additional software on the server. You must also understand Microsoft Internet Information Services (IIS) installation and administration and that of additional add-ons.

The version of the Automation Services package that you deploy to your environment must match the version of the TIBCO Spotfire Server and client that users use to access the server.

Before you install the Automation Services web service, complete the following prerequisite steps.

- Install and configure Windows Server 2008 R2, 2012, or 2012 R2.
- Install and configure Microsoft .NET Framework version 4.5 or later.

  We recommend that you install Microsoft .NET Framework 4.5.2 or later. Make sure to upgrade to the latest version of Microsoft.NET Framework 4.5.
- Set ASP.NET 4.030319 to Allowed on IIS.
- For Windows Server 2012 and 2012 R2, enable Microsoft .NET Framework 3.5. See *Microsoft .NET Framework 3.5 Deployment Considerations* at https://technet.microsoft.com/en-us/library/dn482066.aspx and *Enable .NET Framework 3.5 by using the Add Roles and Features Wizard* at https://technet.microsoft.com/en-us/library/dn482071.aspx for more information.
- Install Java on the server running the jobs. (The Remap Information Services Catalogs and Schemas task require Java.)

For more information about installing or configuring IIS or IIS add-ons, see the documentation for those programs or visit the Microsoft support web site.

Allowing ASP.NET 4.030319 in Internet Information Services

Before you install Spotfire Automation Services, you must configure IIS to allow ASP.NET 4.030319. Perform this task on the computer running a supported version of Windows Server, where you plan to install Spotfire Automation Services.

Prerequisites

Microsoft IIS is installed, and you have administrative access to its configuration. You have reviewed and met the requirements listed on the TIBCO Spotfire System Requirements web page, http://support.spotfire.com/sr_spotfire_main.asp.

Procedure

1. From the **Start** menu, click **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the Console Tree, select the server.
3. In the **IIS** area of the IIS Manager main window, double-click **ISAPI and CGI Restrictions**. The ISAPI and CGI Restrictions pane is displayed.
4. Ensure that **ASP.NET 4.0.30319** appears in the list and its restriction is set to **Allowed**.

   If you are running Windows Server 2008 R2, and if ASP.NET 4.0.30319 is not present, open a command prompt, and at the prompt, run the following command: `C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe /i`, and then return to Step 1.

Be sure that you use the correct versions of each application. Newer versions, if available, might not work as expected.

Installing the Automation Services web service

After you have met the prerequisites for installing TIBCO Spotfire® Automation Services, run its installer.
Perform this task on the computer running a supported version of Windows Server, where you have installed the prerequisite software and tools.

Prerequisites

See Prerequisites for the complete list.

Procedure

1. Create a temporary directory on the server, and in this directory, copy all files that are in the Automation Services installer kit.
2. From the temporary directory, run `setup.exe`, and complete the wizard steps.

Wizard page	Description and Action
Welcome	Click **Next** to begin the wizard.
License Agreement	Accept the terms to continue.
Destination Folder	Specify the installation path.
IIS Web Application Settings	Specify the name for the Spotfire Automation Services Application and the IIS port.
Configuration for TIBCO Spotfire Server	Specify the URL to a Spotfire Server and credentials that have permission to access the Spotfire Server. If you are using Integrated Windows authentication, leave user name and password blank.
Configuration for Mail	Specify a valid SMTP host and a From email address that Spotfire Automation Services can use to send emails. These settings are required by the Send Mail functionality. After installation, you can modify these settings in the configuration file `<`*`installation directory`*`>\webroot\bin\Spotfire.Dxp.Automation.Launcher.exe.config`.

3. After you run the installer, in the Install Complete page, you can open the installer log file, or click **Finish**.

   If the installation does not succeed, review the installer log file. A common cause of installation failure is that the target computer does not meet the system requirements.

Installing hotfixes

After you finish installing Spotfire Automation Services, and before you continue to configure it, check to see if any hotfixes have been released for the version of Spotfire Server. If hotfixes are available, install them.
Perform this task from the Windows server where you installed Spotfire Server and Spotfire Automation Services.

Prerequisites

You have installed, but you have not yet configured, Spotfire Automation Services.

Procedure

1. Open a web browser and browse to the TIBCO Spotfire Product Hotfixes web site: http://support.spotfire.com/patches.asp.
2. Download the hotfixes that are available and follow the installation instructions that are included with each hotfix package.

   Always make sure that you have installed the latest hotfixes before troubleshooting or reporting any problems to TIBCO Support.

Enabling active scripting

For the Spotfire Automation Services export tasks to work properly with Text Areas, you must enable active scripting on the server running Spotfire Automation Services.
Perform this task in the Spotfire Automation Services installation on the Windows Server.

Prerequisites

You must have administrative access to Spotfire Automation Services on the Windows Server.

Procedure

1. From the Windows Server **Start** menu, open the Local Group Policy Editor (`gpedit.msc`).
2. Under **Local Computer Policy**, expand **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Internet Control Panel** > **Security Page** > **Internet Zone**.
3. Right-click **Allow active scripting** and click **Edit**.
4. In the Allow active scripting dialog, click **Enabled**.
5. In the **Options** area, select **Enable** from the list.

What to do next

If you complete this procedure after you install and configure IIS, you must restart IIS for the changes to take effect.

Disabling antivirus and malware scanning software

For performance reasons, we recommend that you disable the on-access scanning for these types of software packages for folders that are used by Spotfire Automation Services.
You should disable on-access scanning of files in the Spotfire Automation Services `webroot` directory and all its sub-directories. When certain antivirus and malware scanning software packages perform an on-access scan, they modify the files or the attributes of the files that they scan, which results in IIS triggering a restart of the web application. When the web application restarts, clients can no longer receive the status of the jobs that are executing, and then reports them as failed or not loaded.

Prerequisites

You must have administrative access to Spotfire Automation Services on the server.

Procedure

- Exclude the following directories from on-access scans:
  - `<Program Files>\TIBCO\Automation Services\`
  - `C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files`

Client Job Sender

TIBCO Spotfire® Automation Services includes the Client Job Sender tool that you can use to automate jobs that are created by the job builder.

The Client Job Sender tool and associated configuration file can be installed on any computer with HTTP or HTTPS (if configured) connectivity to the Spotfire Automation Services web server. Make sure that both files are in the same directory.

Client Job Sender	File name
Executable	`Spotfire.Dxp.Automation.ClientJobSender.exe`
Configuration file	`Spotfire.Dxp.Automation.ClientJobSender.exe.config`

The Spotfire Automation Services Client Job Sender returns a code reporting if a job succeeded or failed. If the job failed, the return code also returns a message indicating how it failed. The return values are stored in the `ERRORLEVEL` environment variable. The valid return codes are as follows.

Return code value	Return code	Message
0	`Success`	The job succeeded.
1	`CommandLineParameterError`	An incorrect command line parameter was supplied.
2	`ServerExecutionError`	The job failed on the server.
3	`ClientExecutionError`	The client failed to send the job to the server.

For information about how to use the Client Job Sender, see the *TIBCO Spotfire® Automation Services User's Manual*.

Configure Spotfire Automation Services

You can adjust Spotfire Automation Services default settings to improve security and to access a Spotfire Server that has certain authentication features configured. Additionally, you can configure Spotfire Automation Services to control automatic and manual updates.

Encrypt traffic between Spotfire clients and Spotfire Automation Services

You can configure Spotfire Automation Services to encrypt traffic between it and its Spotfire clients.

By default, the Spotfire Automation Services web service is configured to use the non-encrypted HTTP protocol for communication between clients (web browsers) and the web service. If you want to encrypt traffic between clients and Spotfire Automation Services, you can enable an SSL binding on the IIS web site in which the Spotfire Automation Services web service is configured. However if you do this, you must ensure that the SSL certificate that is used to encrypt the traffic, or its certification authority, is trusted by the clients.

> If the SSL certificate is not trusted by the clients, the Spotfire Automation Services web service will not function.

For more information about how to enable SSL in Internet Information Services and how to make clients trust SSL certificates, see the Microsoft Internet Information Services documentation.

Encrypting sections of the automation launcher configuration file

If you added authentication information to Spotfire Server or to an SMTP server in the file `Spotfire.Dxp.Automation.Launcher.exe.config`, you can encrypt this section of the file. Perform this task on the Windows Server where Spotfire Server is installed.

Prerequisites

You must have administrative access to the server.

Procedure

1. Browse to the directory *`<installation dir>`*`\webroot\` (where *`<installation dir>`* is the installation directory for Spotfire Automation Services).
2. Run the tool `Spotfire.Dxp.Automation.Launcher.exe`, appending the argument `/encryptSection` followed by the name of the section.

   For example, to encrypt the section containing login information that is used to authenticate with Spotfire Server, type the following.

   ```
   Spotfire.Dxp.Automation.Launcher.exe
   /encryptSection:"Spotfire.Dxp.Automation/authentication"
   ```

   To encrypt the section containing login information for an SMTP server, type the following.

   ```
   Spotfire.Dxp.Automation.Launcher.exe
   /encryptSection:"spotfire.dxp.automation.tasks/smtp"
   ```

Examples

To decrypt an encrypted section, use the `/decryptSection` argument followed by the name of the section.

```
Spotfire.Dxp.Automation.Launcher.exe
/decryptSection:"Spotfire.Dxp.Automation/authentication"
```

```
Spotfire.Dxp.Automation.Launcher.exe
/decryptSection:"spotfire.dxp.automation.tasks/smtp"
```

Configuring web service authentication

By default, any user who accesses the Spotfire Automation Services web service with a web browser can run the web service. However, for security reasons, you can configure the web service to allow only a limited number of users to access Spotfire Automation Services.
You can configure web service authentication in two steps.

1. Disable Anonymous Authentication.
2. Enable Windows Authentication to the Automation Services Web Service using Internet Information Services Manager.

Perform this task on the Windows Server where Spotfire Automation Services is installed.

Prerequisites

You must have administrative access to the web service.

Procedure

1. From the **Start** menu, click **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. From the Console Tree, select the SpotfireAutomation application.
3. In the **IIS** area, double-click **Authentication**.
4. Set the status of Anonymous Authentication to Disabled, and then set the status of Windows Authentication to Enabled.

What to do next

You must configure Spotfire Automation Services to grant access to certain users.

Granting access to certain users

As part of the task of configuring authentication for Spotfire Automation Services, you must grant access to certain users.
Perform this task on the Windows Server where Spotfire Server and Spotfire Automation Services are installed.

Prerequisites

You must have administrative access to the server.

Procedure

1. Browse to the directory *`<installation dir>`*`\webroot\` (where *`<installation dir>`* is the installation directory for Spotfire Automation Services.
2. Open the web configuration file `Web.config`.
3. In the `<system.web>` element, add the following text.

```
<identity impersonate="false"/>
 <authentication mode="Windows" />
 <authorization>
 <allow users="domain\user1" />
 <allow users="domain\user2" />
 <deny users="*"/>
 </authorization>
```

4. Replace the listings for *`domain\user1`* and *`domain\user2`* (and so on) with the domain and users that are applicable in your organization.

You can add as many users as needed.

Example of allowing one user

The following example allows one user in the domain `serenity`.

```
<identity impersonate="false"/>
 <authentication mode="Windows" />
 <authorization>
 <allow users="serenity\malcolm" />
 <deny users="*"/>
 </authorization>
```

Authentication to Spotfire Server with Integrated Windows Authentication

If your Spotfire Server is configured to use Integrated Windows Authentication, you must configure the Spotfire Automation Services web service to run as a user with login and library permissions to the Spotfire Server.

Setting the Spotfire Automation Services web service user

If Spotfire Automation Services is running Integrated Windows Authentication, you must add a web service user in Internet Information Services.
Perform this task in Internet Information Services Manager on the Windows Server where Spotfire Automation Services is installed.

Prerequisites

You must have administrative access to the web service.

Procedure

1. From the **Start** menu, click **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. From the Console Tree, select **Application Pools**.
3. In the **Application Pools** pane, right-click the **TIBCO Spotfire Automation Services Application Pool**, click **Advanced Settings**, and then edit the **Identity** field.
4. Change the identity to a domain user that has login and library permissions to the Spotfire Server.

What to do next

Spotfire Automation Services Web Service is running as a non-standard user. You must also set user access to full control over files in the Spotfire Automation Services installation folder.

Setting file permisions to the Spotfire Automation Services installation folder

After setting the Spotfire Automation Services web service user, be sure that the specified user has the required file permissions.
Perform this task in Internet Information Services Manager on the Windows Server where Spotfire Automation Services is installed.

Prerequisites

You must set the Spotfire Automation Services web service user. See Setting the Spotfire Automation Services web service user.

Procedure

1. From the **Start** menu, click **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. From the Console Tree, expand the Spotfire Automation Services Web Application.
3. Right-click the `bin` folder, and then click **Edit Permissions**.
4. Select the **Security** tab, and then click **Edit.**
5. In the Permissions for bin dialog, add the user name that you designated to run the Spotfire Automation Services application pool if it is not present, and under **Permissions for Users**, set the permission to allow **Full control**.

What to do next

If you entered a user name and password when you installed Spotfire Automation Services, you must also remove these from the configuration file.

Removing credentials from the Spotfire Automation Services configuration file

After setting the Spotfire Automation Services web service user and assigning file permissions, you must remove from the configuration file any credentials that you set during installation.
Perform this task using a text editor on the Windows Server where Spotfire Automation Services is installed.

Prerequisites

You must have administrative acccess to the Windows Server, and have set file permissions for the Spotfire Automation Services web services user. See Setting file permisions to the Spotfire Automation Services installation folder.

Procedure

1. Using a text editor, browse to and open the file `<`*`installation directory`*`>\webroot\bin\Spotfire.Dxp.Automation.Launcher.exe.config` where `<`*`installation directory`*`>` is the installation directory for Spotfire Automation Services.
2. In the section labelled `authentication`, remove the values for `username` and `password`.

   Leave the `serverUrl` entry as is.

   When you finish editing this line, it should be similar to the following.

```
<authentication serverUrl="http://spotfireserver/"
username="" password="">
```

Authentication to Spotfire Server with client certificates

If your Spotfire Server is set up to use client certificates, you must install the certificate used for authentication on the Spotfire Automation Services server and configure Spotfire Automation Services to use it when authenticating to the Spotfire Server. Then you must configure the access rights to the certificate so that the network service account has access.

See the *TIBCO Spotfire® Server Installation and Configuration Manual* for more information about client certificates.

Installing a client certificate

The first step of using Spotfire Automation Services with client certificates is installing the client certificate.
Perform this task on the Windows Server where Spotfire Automation Services is installed.

Prerequisites

You must have administrative access to the web service, and you must have access to the certificate that you want to install.

Procedure

1. From the Windows **Start** menu, in the search box, type `MMC`.
   The Microsoft Managment Console starts.
2. Click **File** > **Add/Remove Snap-in**.
3. From the list, select **Certificates**, and then click **Add**.
4. Select the option to manage certificates for the Local computer.
5. Install the certificate in the **Personal** container.
6. In the Microsoft Management Console, right-click the installed certificate, and then click **All Tasks\Manage Private Keys**.
7. Grant the user NETWORK SERVICE access rights to the certificate.

What to do next

After installing the certificate and granting the user access rights, you must configure Spotfire Automation Services to use the client certificate.

Configuring Spotfire Automation Services to use a client certificate

After you install the client certificate, you must configure Spotfire Automation Services to use the certificate.

Perform this task using a text editor on the Windows Server where Spotfire Automation Services is installed.

Prerequisites

You must have administrative access to the web service.

Procedure

1. Using a text editor, browse to and open the file `<installation directory>\webroot\bin\Spotfire.Dxp.Automation.Launcher.exe.config` where `<installation directory>` is the installation directory for Spotfire Automation Services.
2. In the section labelled `certificate`, if the section is commented out, remove the comment markers.
3. Set `useCertificates` to `true`, and then set `storeName`, `storeLocation`, and `serialNumber` to match the installed certificate.

Example

```
<Spotfire.Dxp.Automation>
 <authentication
 serverUrl="https://spotfireserver.yourorganization.com">
 <!-- <proxy username="" password="" /> -->
 <certificates
 useCertificates="true"
 storeName="MyStore"
 storeLocation="LocalMachine"
 serialNumber="00AABB11CCDD2233DD" />
 </authentication>
</Spotfire.Dxp.Automation>
```

Control embedding behavior of data function-based data sources

You can use Spotfire Automation Services jobs to save analyses containing data function-based data sources (for example, all on-demand data tables). However, these data sources are not loaded automatically by default, but must be manually refreshed. You can set Spotfire Automation Services to control this behavior.

Modifying the force update behavior for embedded data

You can control the force-update behavior by modifying the configuration file in Spotfire Automation Services.
Perform these tasks using a text editor on the computer where Spotfire Automation Services is installed.

Prerequisites

You must have administrative access to the web service on the Windows server.

Procedure

1. Using a text editor, browse to and open the file `<installation directory>\webroot\bin\Spotfire.Dxp.Automation.Launcher.exe.config` where `<installation directory>` is the installation directory for Spotfire Automation Services.
2. Find the entry `saveAnalysis` and set the force update behavior to either `true` or `false`:
   ```
   <saveAnalysis forceUpdateBehaviorManualWhenEmbeddingData="false"/>
   ```
3. Save the changes in `Spotfire.Dxp.Automation.Launcher.exe.config`.
4. Restart the Spotfire Automation Services application pool.

Modifying the force update setting for a specific TIBCO Spotfire Professional installation

If you want to test jobs by executing them locally, you can modify this setting on your own TIBCO Spotfire® Professional computer using these steps.
Perform these tasks on the computer where Spotfire Professional is installed.

Prerequisites

Because the directory `C:\Program Files (x86)\TIBCO\Spotfire\7.0.0\Modules\` is hidden by default, you must set your Windows Explorer options to show hidden files and folders.

Procedure

1. Open the Forms file `C:\Program Files (x86)\TIBCO\Spotfire\7.0.0\Modules\Spotfire.Dxp.Main.dll.config`.

   For example, `C:\Program Files (x86)\TIBCO\Spotfire\7.0.0\Modules\Spotfire DXP Forms_9.14.5830.4061`.
2. Find the node `<configuration><configSections>` and add the following.
   ```
   <sectionGroup
    name="spotfire.dxp.automation.tasks">
    <section name="saveAnalysis"
    type="Spotfire.Dxp.Automation.Tasks.SaveAnalysisSettings,
    Spotfire.Dxp.Automation.Tasks,
    Version=3.0.2736.26364,
    Culture=neutral,
    PublicKeyToken=789861576bd64dc5"
   ```

```
 requirePermission="false" />
</sectionGroup>
```

3. Anywhere inside the topmost `<configuration>` node, add the following.

   ```
   <spotfire.dxp.automation.tasks>
   <saveAnalysis forceUpdateBehaviorManualWhenEmbeddingData="false"/>
   </spotfire.dxp.automation.tasks>
   ```

4. Restart Spotfire Professional to use the new settings.

Upgrading Spotfire Automation Services web service

To install an upgrade to your installation of Spotfire Automation Services, you must complete upgrading tasks for the web service, the job builder, and the command-line client.
Perform this task on the Windows Server where Spotfire Automation Services is installed.

During the installation, the following upgrades are applied:

- Job Builder
- Command-line client

Prerequisites

You must have administrative access to the Windows Server.

Procedure

1. On the Windows Server, browse to the directory `<installation directory>\webroot\bin`.
2. Make a copy of the file `Spotfire.Dxp.Automation.Launcher.exe.config.`

   > Use this copy of the file to refer to as you are configuring the new version of the configuration file.

3. Make copies of any deployed custom extensions and the file `AddIns.xml`.
4. Uninstall the previous Spotfire Automation Services web service.
5. Install the new version of Spotfire Automation Services web service by running `setup.exe` on the computer that hosts the web server.

   Follow the instructions in the installation wizard.
6. Configure the new installation of Spotfire Automation Services, providing required encryption and authentication.

   > View the old `Spotfire.Dxp.Automation.Launcher.exe.config` next to the new version so that you can copy the necessary settings from the old file to the new file.

Deploying extensions

If you create an extension, you must deploy it to TIBCO Spotfire® Automation Services to enable it to run.
Perform this task on a Windows Server that has TIBCO Spotfire® Professional client, Spotfire Server, and Spotfire Automation Services installed.

Prerequisites

You must have a working extension in your Spotfire Professional client. You must have administrative access to Spotfire Automation Services on the Windows Server.

Procedure

1. In the Spotfire Professional installation, locate the directory `<installation location>\Modules\<module>`, where `<installation location>` is the path including the version number, and `<module>` is the directory for the extension you want to copy.

   For example, `c:\Program Files (x86)\TIBCO\Spotfire\7.0.0\Modules\MyExtension_1.0.0`.

   By default, in the Windows user interface, the folder `Modules` is hidden. If you do not see this folder, set your Windows options to view hidden folders.

2. In the extension directory, copy to your clipboard all files that are needed to run the extension except the file `modules.xml`.
3. In the Spotfire Automation Services installation, find the directory `webroot\bin`, and paste the copied extension files there.
4. Return to the module directory in the Spotfire Professional installation as described in Step 1, and, using a text editor, open the file `module.xml`.
5. In the extension's file that is named `module.xml`, find the section that is named `<extensions>` and copy it to your clipboard.

   Copy the entire section, including the XML tags `<extensions>` and `</extensions>`.

6. Return to the Spotfire Automation Services directory `webroot\bin`, and then find and open in your text editor the file `AddIn.xml`.
7. In the file `AddIn.xml`, find the section that is named `<AddInRegistry>`, and paste the `<extensions>` section you copied into this section.

   The files `module.xml` in Spotfire Professional and `AddIns.xml` contain different letter cases. You must replace all occurrences of *`addIn fullTypeName`* with *`AddIn FullTypeName`*.

8. Save the changes to `AddIn.xml`.

Verifying the job builder license

Before users can use the Spotfire Automation Services job builder, an administrator must grant them a license in Spotfire.
Perform this task from a Windows computer running Spotfire. For more information about assigning licenses, see the *TIBCO Spotfire® Deployment and Administration Manual*.

Prerequisites

You must have administrative access to Spotfire Server.

Procedure

1. Start Spotfire, logging in with a user account that has administrator user rights.
   a) If prompted, download all updates from the Spotfire Server.
   Spotfire restarts after the update is downloaded and installed.
2. From the Spotfire menu, click **Tools** > **Administration Manager**, and then select the tab **Groups and Licenses**.
3. In the **Available groups** list, select a group.
4. Click the **Licenses** tab.
5. Expand the TIBCO Spotfire Extensions license entry.
   The list of extensions appears. This list includes Automation Services Job Builder Tool.
6. Ensure that licenses for both Addess to Extensions and Automation Services Job Builder Tool are selected (indicated by a green check mark).
   a) If either or both are not selected, click **Edit**.
   b) In the Licenses for group dialog, expand the TIBCO Spotfire Extensions license entry.
   c) Select the check boxes for **Access to Extensions** and **Automation Services Job Builder Tool**, and then click **OK**.
7. Repeat Step 3 through Step 6 for each group of users that should be permtted to use Automation Services.

Deploying the Automation Services job builder

If your server users require the Automation Services job builder functionality, you must deploy it to the Spotfire Server.
Perform this task on a Windows computer that has TIBCO Spotfire® installed.

Prerequisites

You must have administrative access to Spotfire Server.

Procedure

1. From a web browser, open the Spotfire Server Administration Console located at `http://`*`spotserver`*`/spotfire/administration` (where *`spotserver`* is the name of the Spotfire Server).
2. Log in to the Spotfire Server as a Spotfire administrator.
3. Select the **Deployment** tab and then, from the **View** list, select a deployment area that contains a valid Spotfire deployment. Click **Add**.

   > You must select a deployment area that contains `SpotfireDXP.sdn`.

4. In the Add to Deployment dialog, click **Browse**.
5. In the File Upload dialog, find and select the package file `AutomationServices.spk`.
6. In the Add to Deployment dialog, click **OK**.
   The file is uploaded and added to the distrubtion, and the list of packages is updated with the contents of the file.
7. Click **Validate** to ensure that the deployment has been completed successfully and is valid.
8. Click **Save** to save and publish the deployment.
   a) In the Save Deployment dialog, type a version number and description for the deployment, and then click **OK**.
9. Restart Spotfire and log in as usual.
   The Spotfire client downloads the new client package.

Troubleshoot Spotfire Automation Services

If Spotfire Automation Services is not configured correctly, users cannot run jobs on the server. In this case, Spotfire Automation Services displays an error message that directs the user to contact the Spotfire administrator.

Configuring the Automation Services log file

If users see an error message when they try to run jobs using Spotfire Automation Services, you must review the file `<installation directory>\LogFiles\Spotfire.Dxp.Automation.log` directory to discover the problem. Configuring Spotfire Automation Services to write to the log file is a required step for such troubleshooting.
All configurations for Spotfire Automation Services, including the log file configuration, are performed in the file `<installation directory>\webroot\bin\Spotfire.Dxp.Automation.Launcher.exe.config` .

Prerequisites

You must have administrative access to the web service.

Procedure

1. Using a text editor, open the file `<installation directory>\webroot\bin\Spotfire.Dxp.Automation.Launcher.exe.config`.
2. Update the sections of the configuration file to contain the correct URL for the Spotfire Server, the host name of the SMTP server, or other settings to correctly reflect the service.

Configuration file extract

```
<--
If username and password are empty or doesn't exist, then we
 login using the current Windows account (using Windows
 Authentication).

 serverUrl (Required): The url to the Spotfire Analytics Server
 "http[s]://<server>[:port]/"
 username: The spotfire user to authenticate with.
 password: The password to authenticate with.

proxy (you need to set the
 system.net/defaultProxy/proxy: proxyaddress
 to use it if you run under a system account (from
 web sites etc.)):

username: Proxy username for communication between web server
 and Spotfire Analytics Server.
 password: Proxy password for communication between web server
 and Spotfire Analytics Server.


certificates (Certificates to use when authenticating
 with Analytics Server):
 useCertificates (false): Should we use certificates
 storeName (TrustedPeople): The store name to get the
 certificates from.

[AddressBook|AuthRoot|CertificateAuthority|Disallowed
 |My|Root|TrustedPeople|TrustedPublisher]

storeLocation (LocalMachine): [CurrentUser|LocalMachine]
 The location to take the certificates from.

serialNumber: The serial number of the certificate to use.
-->

<authentication
 serverUrl="http://spotserver/"
 username=""
 password="">
```

Library import conflict mode

When a user opens Spotfire Automation Services job builder to configure **Import Library Items** and selects the option **Include permissions**, the files are moved, instead of copied, from the source directory.

The files are moved because you defined the import task to adhere to the conflict resolution mode option **keep new**, and a GUID conflict causes the operation. Because the newest file versions are in the target directory, the files in the source directory are not retained.

Uninstalling Spotfire Automation Services

You uninstall Spotfire Automation Services using the standard Windows tools for uninstalling software.
Perform this task on the Windows Server where Spotfire Automation Services is installed.

Procedure

1. Open the Control Panel and click **Program and Features**.
2. Find and double-click the entry TIBCO Spotfire® Automation Services.
   Spotfire Automation Services is removed from the server and the added Internet Information Services configuration is removed. Some files might remain in the installation folder after uninstallation is complete.
3. Open the folder *`<installation directory>`* and delete any remaining files.